KATHOLISCH
Bistum Mainz

01

# [Merkblatt Einführung zum kirchlichen Datenschutz]

## einfach & sicher

Datenschutz im Bistum Mainz

Betriebliche Datenschutzstelle
Stand: Juli 2022

# Merkblatt
# Einführung zum kirchlichen Datenschutz

**Nicht nur Behörden und sonstige Stellen von Bund und Länder verarbeiten personenbezogene Daten, sondern auch die Kirchen und kirchliche Einrichtungen. Aufgrund des verfassungsrechtlich garantierten Selbstbestimmungsrechtes von Religionsgemeinschaften findet allerdings weder die DS-GVO noch das BDSG auf Kirchen und kirchliche Einrichtungen Anwendung. Um dennoch dem Recht des Einzelnen auf informationelle Selbstbestimmung Rechnung zu tragen, haben die Kirchen jeweils eigene datenschutzrechtliche Regelungen geschaffen.**

Für die Bistümer der katholischen Kirche trat das **„Gesetz über den kirchlichen Datenschutz (KDG)“** am 24. Mai 2018 in Kraft. Hier erfolgte eine umfassende Novellierung und Anpassung an die DS-GVO.

Wichtig: Der Anwendungsbereich des KDG erstreckt sich auch auf sonstige kirchliche Einrichtungen und Werke wie Stiftungen, Anstalten und Verbände (z.B. Caritas). Es ist also stets im Einzelfall zu prüfen, ob eine Einrichtung den kirchlichen Datenschutzregelungen unterliegt.

Das KDG hebt hervor, dass der besondere Schutz des Beicht- und Seelsorgegeheimnisses von den datenschutzrechtlichen Bestimmungen unberührt bleibt. Daher gilt, dass unabhängig von den datenschutzrechtlichen Möglichkeiten eine wie auch immer geartete Nutzung der anvertrauten Information unzulässig ist.

Darüber hinaus ist jeweils die Bestellung eines kirchlichen Datenschutzbeauftragten vorgesehen.

## Überblick über die wesentlichen Regelungen des KDG:

### 1. Anwendungsbereich des KDG

Das KDG findet auf die Verarbeitung personenbezogener Daten durch

- die Diözese,
- die Kirchengemeinden,
- die Kirchenstiftungen,
- die Kirchengemeindeverbände,
- den Caritasverband und die entsprechenden Untergliederungen und Fachverbände sowie
- sonstige kirchliche Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und Rechtsträger

Anwendung.

Auf die konkrete Art der Datenverarbeitung kommt es dabei nicht an. Im Ergebnis ist der Anwendungsbereich des KDG damit sehr weit.

Im Einzelfall ist zu prüfen, ob besondere kirchliche oder staatliche Rechtsvorschriften die Verarbeitung personenbezogener Daten einschließlich deren Veröffentlichung regeln oder vorschreiben. Ist dies der Fall, gehen Sie den Vorschriften des KDG vor (Anwendungsvorrang), wenn und soweit das Schutzniveau des KDG nicht unterschritten wird (§2 Abs. 2 KDG).

## 2. Begriffsbestimmungen

Die maßgeblichen Begriffsbestimmungen finden sich in § 4 KDG, wobei auch hier eine Anlehnung an die entsprechenden Begriffsbestimmungen der DS-GVO erfolgte. Ergänzend sind Beschäftigte (Nr. 24) ausführlich und beispielhaft erläutert.

## 3. Grundsätze der Datenverarbeitung

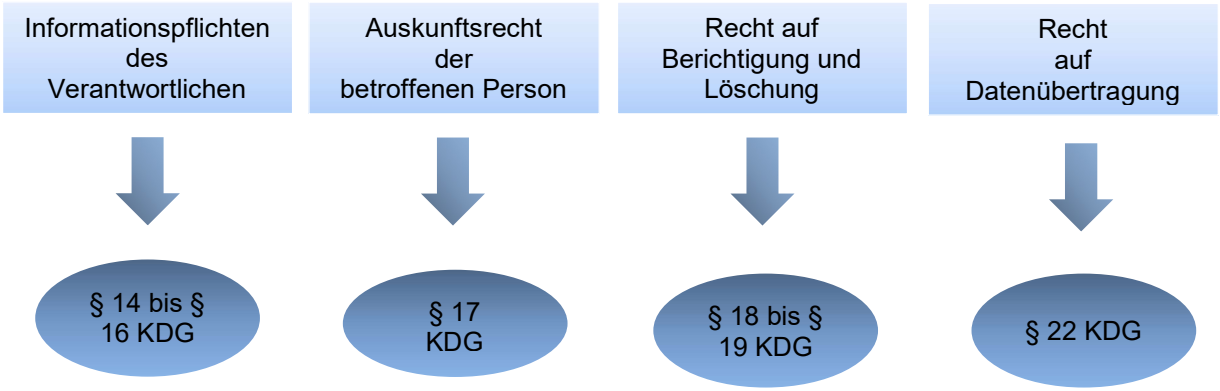
§ 5 des KDG enthält eine ausdrückliche Regelung zum Datengeheimnis, so dass auch bei katholischen Einrichtungen an der Praxis der schriftlichen Verpflichtung der Beschäftigten auf das Datengeheimnis festgehalten wird. Im Übrigen enthalten die Regelung des Kapitels 2 KDG viele Vorgaben, die sich ähnlich in der DS-GVO und dem BDSG wiederfinden, also insbesondere

- die Grundsätze der Datenverarbeitung in § 7 KDG,
- Vorgaben zur Rechtmäßigkeit der Datenverarbeitung einschließlich der Zweckänderung in § 6 KDG,
- Anforderung an die Einwilligung der Betroffenen (§ 8 KDG) sowie
- Voraussetzung der Offenlegung und Übermittlung personenbezogener Daten an kirchlichen öffentliche Stellen sowie Dritte (§§ 9 und 10 KDG).

Dem Schutz besonderer Kategorien personenbezogener Daten trägt das KDG ebenfalls Rechnung. Die Verarbeitung ist grundsätzlich untersagt und nur in Fällen des §11 Abs. 2 KDG zulässig. Die Definition der besonderen Kategorien personenbezogener Daten findet sich in § 4 Nr. 2 KDG, wobei auch hier wieder die Zugehörigkeit zu einer Kirche oder eine Religionsgemeinschaft nicht dazu zählt.

## 4. Rechte des Betroffenen

Die Rechte des Betroffenen finden sich in Kapitel 3, unter anderem:



## 5. Der Datenschutzbeauftragte

Jede Kirchengemeinde, Kirchenstiftung und jeder Kirchengemeindeverband muss einen betriebl. Datenschutzbeauftragten bestellen (§ 36 Abs. 1 KDG). Bei allen anderen Einrichtungen und Rechtsträgern hängt die Bestellung davon ab, ob

- in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, oder aber
- die Kerntätigkeit in sensiblen Verarbeitungsvorgängen oder in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht (§ 36 Absatz 2 lit. b und c KDG).

Ist ein betrieblicher Datenschutzbeauftragter bestellt, ist dieser weisungsfrei und besonders geschützt (§ 37 KDG). Seine Aufgaben ergeben sich aus § 38 KDG.

Leitender Betrieblicher Datenschutzbeauftragter
Wolfgang Knauer, Tel. 06131/253-889

Gemeinsame Betriebliche Datenschutzbeauftragte
für die Kirchengemeinden
Michaela Beiersdorf, Tel. 06131/253-821

Datenschutzkoordinatorin
Alexandra Glinka, Tel. 06131/253-857

Bischöfliches Ordinariat Mainz
Betriebliche Datenschutzstelle
Weißliliengasse 2d, 55116 Mainz
Postfach 1560, 55005 Mainz
datenschutz@bistum-mainz.de

## 6. Diözesandatenschutzbeauftragte

Im Anwendungsbereich des KDG obliegt die Datenschutzaufsicht dem jeweiligen Diözesandatenschutzbeauftragten (§ 42 ff. KDG). Es gibt also im Bereich der katholischen Stellen und Einrichtungen eine regionale Aufsicht.

### Zuständigkeit Mittel- und Südwestdeutsche Bistümer

Diözesandatenschutzbeauftragte
Ursula Becker-Rathmair

Katholisches Datenschutzzentrum Frankfurt
für Erzbistum Freiburg, Bistum Fulda, Bistum Limburg, Bistum Mainz, Bistum Rottenburg-Stuttgart, Bistum Speyer, Bistum Trier
Roßmarkt 23
60311 Frankfurt am Main
Tel.: 069 58 99 755-10
Fax: 069 58 99 755-11
E-Mail: info@kdsz-ffm.de
www.kath-datenschutzzentrum-ffm.de

# 1.0 Datenschutzklassen

## 1.1 Datenschutzklasse I

Zur Datenschutzklasse I gehören Daten, deren Missbrauch keine besondere Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören Adressangaben, Berufs-, Branchen- oder Geschäftsbezeichnungen. Für sie sind die unter Ziffer 2.1 festgelegten Maßnahmen durchzuführen.

## 1.2 Datenschutzklasse II

Zur Datenschutzklasse II gehören Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen können. Hierzu gehören Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten, etc. Für sie sind die unter Ziffer 2.2 festgelegten Maßnahmen durchzuführen.

## 1.3 Datenschutzklasse III

Zur Datenschutzklasse III gehören Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen können. Hierzu gehören Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen, etc. Für sie sind die unter Ziffer 2.3 festgelegten Maßnahmen durchzuführen.

## 1.4 Nicht zu speichernde Daten

Daten, deren Kenntnis dem Beicht- oder Seelsorgegeheimnis unterliegen, sowie Daten über die Annahme einer Person an Kindes Statt (Adoptionsgeheimnis), sind in besonders hohem Maße schutzbedürftig. Ihre Ausspähung würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen. Daher dürfen diese Daten nicht auf Arbeitsplatzcomputern verarbeitet werden.

## 1.5 Einordnung in die Datenschutzklassen

Bei der Einordnung der zu speichernden personenbezogenen Daten in die vorgenannten Schutzklassen, ist auch deren Zusammenhang mit anderen gespeicherten Daten, der Zweck ihrer Verarbeitung und das anzunehmende Missbrauchsinteresse zu berücksichtigen.

## 1.6 Geltung der jeweils höchsten Schutzklasse

Gehören die auf einem Arbeitsplatzcomputer gespeicherten Daten unterschiedlichen Schutzklassen an, so richten sich die nach dieser Richtlinie zu treffenden Maßnahmen nach der höchsten, in der Datenverarbeitung vorkommenden Schutzklasse.

## 1.7 Vermeidung der Mehrfachsicherung

Schutzmaßnahmen nach den Datenschutzklassen II oder III machen die für die jeweils niedrigeren Schutzklassen vorgesehenen Maßnahmen gleicher Zielrichtung in der Regel entbehrlich.

## 2.0 Nach den Datenschutzklassen erforderliche Maßnahmen

### 2.1 Maßnahmen in Datenschutzklasse I

Zum Schutz der in die Datenschutzklasse I einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

- Die Inbetriebnahme des PC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich, das in regelmäßigen Abständen erneuert werden sollte. Im Mehrbenutzer- oder Netzwerkbetrieb und bei einer PC/Host-Koppelung ist zudem eine Rechteverwaltung auf Unterverzeichnis- und Dateiebene erforderlich, wenn nicht alle Nutzer berechtigt sein sollen, auf die personenbezogenen Daten Zugriff zu nehmen.
- Sicherungskopien und Ausdrucke der Datenbestände sind verschlossen, im Interesse der Dienststelle möglichst in feuerfesten Stahlschränken, aufzubewahren.
- Nicht mehr benötigte Dateien sind so zu löschen, dass ihre Wiederherstellung ausgeschlossen ist (physikalisches Löschen).

### 2.2 Maßnahmen in Datenschutzklasse II

Zum Schutz der in die Datenschutzklasse II einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

- Die auf der Festplatte gespeicherten Programme und Daten sollten dauerhaft so verschlüsselt werden, dass eine Entschlüsselung nur bezüglich solcher Programmteile und Daten stattfindet, die vom PC in den Hauptspeicher geladen werden (Online-Verschlüsselung). Der Zugang zum Entschlüsselungsprogramm ist nur nach Eingabe einer Benutzerkennung und eines Passwortes möglich, das vom Anwender in regelmäßigen Abständen zu erneuern ist. Dabei ist eine Begrenzung der Anmeldeversuche erforderlich. Anmeldeversuche am PC sind durch Einsatz geeigneter Programme zu protokollieren.
- bei Mehrbenutzer- und Netzwerkbetrieb ist eine abgestufte Rechteverwaltung für jeden Benutzer oder einzelne Benutzergruppen erforderlich. Der Zugang zum Betriebssystem sollte nur für den Systemverwalter möglich sein.
- Sicherungskopien sollten ebenfalls verschlüsselt und in abschließbaren, feuerfesten Schränken aufbewahrt werden; die Schnittstellen sind vor unberechtigtem Zugriff zu sichern.

### 2.3 Maßnahmen in Datenschutzklasse III

Zum Schutz der in die Datenschutzklasse III einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

- Die auf der Festplatte gespeicherten Programme und Daten sind dauerhaft zu verschlüsseln (Online-Verschlüsselung). Eine Entschlüsselung findet nur bezüglich solcher Programmteile und Daten statt, die vom PC in den Hauptspeicher geladen werden. Der Zugang zum Entschlüsselungsprogramm ist nur nach Eingabe einer Benutzerkennung und eines zumindest achtstelligen Passwortes möglich, das vom Anwender in regelmäßigen Abständen zu erneuern ist. Trivialpasswörter (z.B. 4711, 12345, Gast, Master) dürfen nicht verwendet werden. Dabei ist programmseitig eine Begrenzung der Anmeldeversuche auf höchstens drei Fehlversuche vorzusehen. Im Mehrbenutzer- und Netzwerkbetrieb sind für jeden Benutzer abgestufte Rechte für den Zugriff auf Programme, Daten und Peripheriegeräte (insbes.

Laufwerke, Schnittstellen) durch einen Systemverwalter zu vergeben; Systemaktivitäten sind durch eine hierfür geeignete Software zu protokollieren, deren Auswertung durch eine Person erfolgen sollte, die selbst nicht Systemverwalter ist.

- Sicherungskopien sind zu verschlüsseln und in verschlossenen, möglichst feuerfesten Stahlschränken aufzubewahren.

## Impressum:

Herausgegeben vom
Bischöflichen Ordinariat Mainz

Betriebliche Datenschutzstelle im Bistum Mainz
☎ 06131-253857
✉ Postfach 1560, 55005 Mainz
datenschutz@bistum-mainz.de

**Redaktion:** Wolfgang Knauer, Alexandra Glinka